How to Request Azure Resource Access (PIM/JIT)

Modified on: Wed, 2 Mar, 2022 at 12:50 PM

TABLE OF CONTENTS

Introduction

This is the Step-by-step process to request access to subscription resources. Primarily attended for reference refresher after training.

Definitions

PIM/JIT Permissions

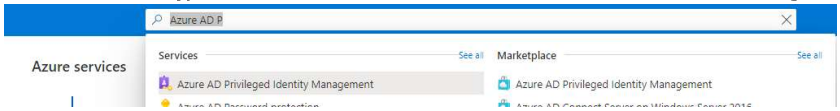
It's necessary to have a base understanding of the PIM/JIT roles you need and when you need them. Below is a high level explanation of these roles

- **SQL DB Contributor**
  - Required to make changes to an EP (Elastic Pool) or DB from the Azure portal (expanding EP/DB size, writing SQL to a specific DB)
- **Virtual Machine Contributor**
  - Required to make changes to a Virtual Machine from the Azure portal
- **Network Contributor**
  - Required to make major network changes to a subscription from the Azure portal
    - Add/change NSG
    - Add/change VPN (uplift GW)
    - There are more items to add, but this should provide a starting point for understanding
- **NetworkWatcher-Troubleshoot**
  - Does not require PIM request
  - Allows for basic Network troubleshooting functionality without needing full network contributor or NetworkWatcher-FullPerm
  - Some of the tests included are IpFlowVerify, Network Config Diagnostic, Connectivity check, etc..
- **NetworkWatcher-FullPerm**
  - Does require PIM request
  - Allows for the creation of network watcher connection tests, packet captures, etc.. Includes virtual machine and extension write to allow for the deployment of the network watcher extension if required. Also includes SAS permission for the storage of packet capture logs.
  - Some of the tests included are IpFlowVerify, Network Config Diagnostic, Connectivity check, etc..
- **Contributor**
  - This is the role that grants blanket access to a subscription including creating resources. We should use it the least.
- **Virtual Machine JIT Login – Internal**
  - This is your go to roles for VM access within a sub and it is more common. You'll need it to gain remote access to an endpoint within a sub and with it you can navigate to all VM's in a specific sub

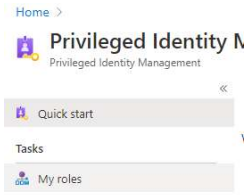
Steps

1. Log onto the Thoughtonomy Ltd portal in Azure

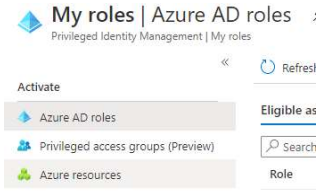
2. Go to Home and Type "Azure AD P" in the main search bar. then click on "Azure AD Privileged Identity Management".



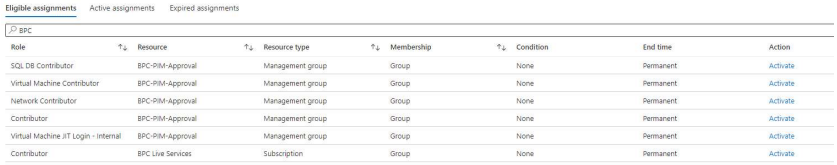
3. Click on "My Roles".



4. Click on "Azure Resources".

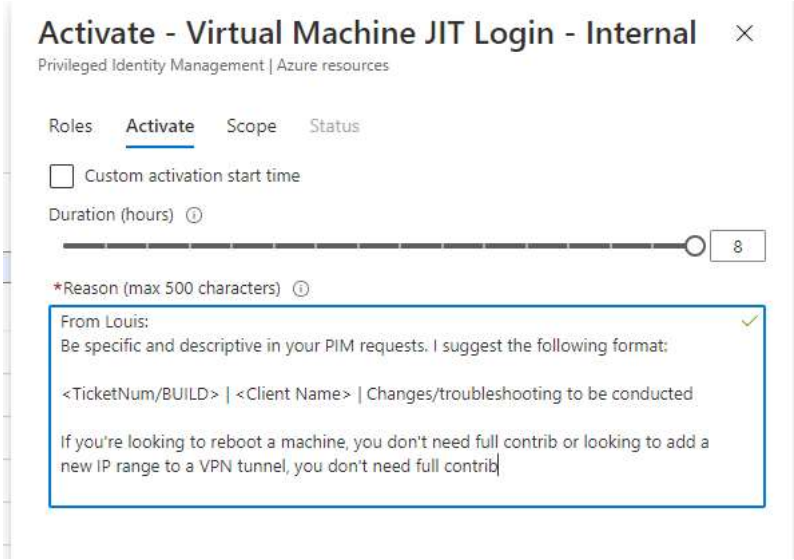


5. Type "BPC" in the search bar.

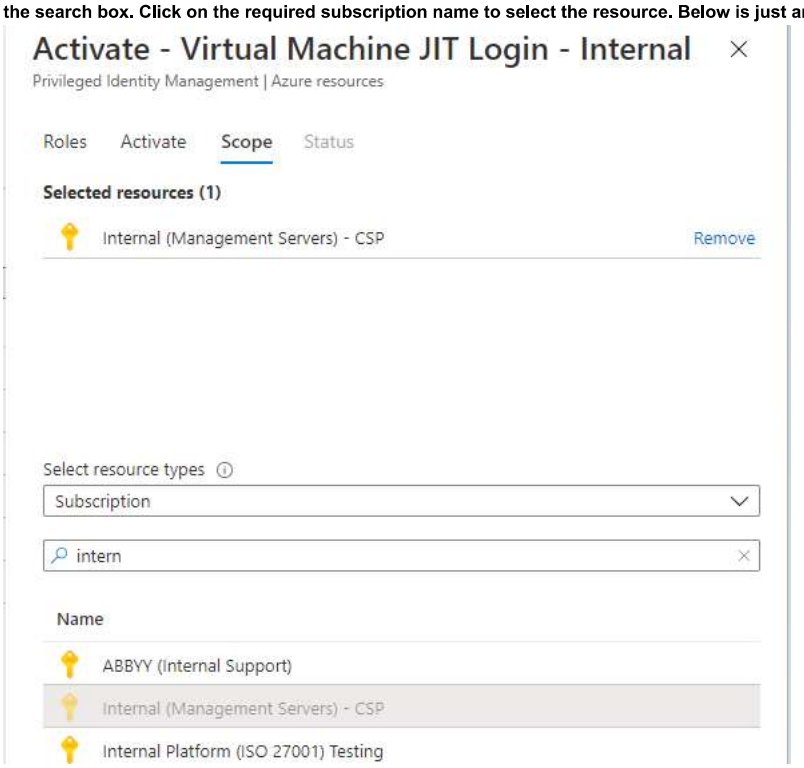


6. Select the required Role(s) and click "Activate on the far right Action Column.

7. Type in a quick explanation and copy/paste the support case URL.



8. Click on the Scope tab next to the Activate tab. Then start typing the subscription name(desired subscription) which you are working on, until the name shows up below the search box. Click on the required subscription name to select the resource. Below is just an example.

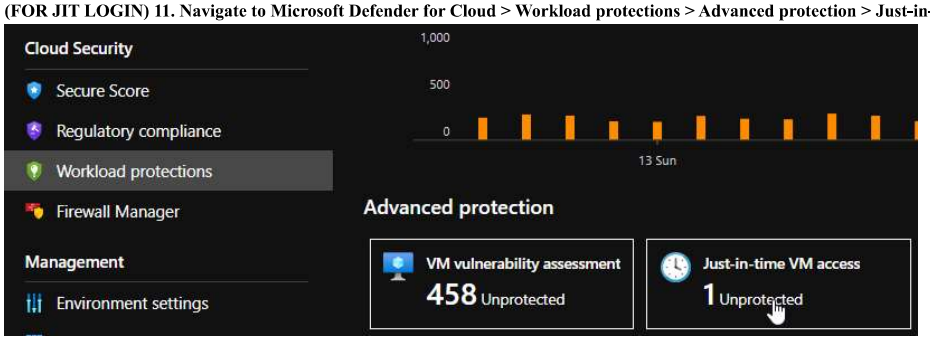


9. Click on the Activate button at the bottom of the window.

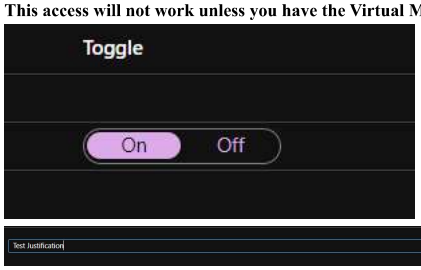
10. Wait for approval or mention PIM approval required in your Ops group.

```
NOTE: Please check that you have access to the appropriate Key Vault. You will need this information to be able to authenticate to subscription's resou
```

(FOR JIT LOGIN) 11. Navigate to Microsoft Defender for Cloud > Workload protections > Advanced protection > Just-in-time VM access



12. Select the checkbox on the left & select the "Request access" command button. Toggle "On" and enter a justification in the lower-most input box, then click the Open ports button. This will create a temporary NSG rule to allow for port 3389 access from your host's Public IP address to the Management Server of your selected subscription.
This access will not work unless you have the Virtual Machine JIT Login - Internal role.



13. You will now be able to broker a connection to the customer environment using the credentials found within our Azure Key Vault, after following the Key Vault Access doc in

Preview